Influence of Social Networks on Cyber Security

Kate Coronges, MPH, PhD

Network Science Center (NSC) & Behavioral Sciences and Leadership (BS

COL Ron Dodge, PhD, Information & Education Technology
Alysse Pulido, Behavioral Sciences & Leadership

Sunbelt XXXII, Redondo Beach, CA
March 13-18, 2012

Sponsored by Army Research Institute (ARI) #10086985

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
18 MAR 2012	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Influence of Social Networks on Cyber Security	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **US Military Academy Network Science Center, and Dept of Behavioral Sciences & Leadership West Point, NY 10996**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**22**	

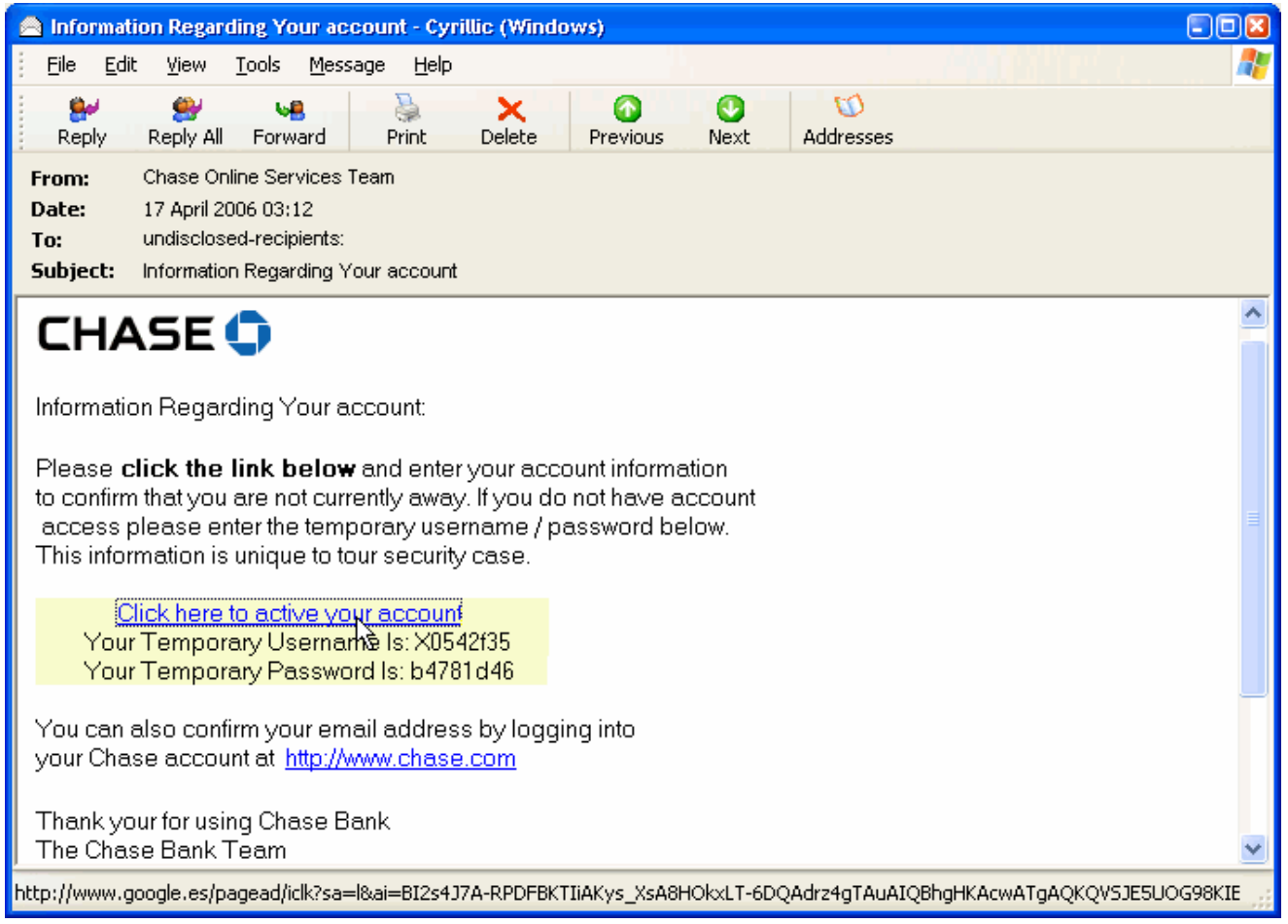
Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Study Objective

- Examine cadet social networks at the US Military Academy to identify network metrics and processes associated with security vulnerabilities.
- Identify social mechanisms to improve security among college aged cadets at the US Military Academy at West Point.
- Compare processes between formal versus informal networks.

What is Phishing

- Phishing is a form of electronic deception in which an attacker tries to obtain personal information by mimicking a trustworthy entity.



Background

- Phishing attacks are becoming widespread and costly - $2.4M-$9.4M in fraud losses per year
- Future military officers are especially vulnerable – access to sensitive data.
- Phishing threaten personal and national security
- Younger generations are more susceptible - more trustworthy and less fearful of technology.
- Homophily around risky behaviors exists among friends but not clear evidence for organizational links.

Study Design

Part of a large scale Army-wide initiative to evaluate security training

- Training Assessment Study (n=894)
  - Send false phishing emails out to students
  - Longitudinal design – 3 time points over 1 year
  - 9 military units assigned to 1of 3 conditions: (1) no notification, (2) notification, (3) given a 10-minute training module online
  - Findings showed that upper classmen, females and those in cond2 had the greatest reduction in phishing failures (Results published CISSE, 2011)

Social Network Study (n=128)

Network Data

– *INFORMAL NETWORK*
Friendships: “Who do you consider a friend within the company”

– *FORMAL NETWORK*
Chain of command: immediate supervisorial chain

Dependent Variables

– *PHISHING BEHAVIOR*: Detect whether student clicked the embedded link, and entered credentials

– *WARNING ACTIVITY*: Warn another cadet within the company (paper survey)

Analysis:

Correlations & Logistic regression

→ *centrality*

→ *network exposure (# alters that show phishing and warning behaviors)*

Participants

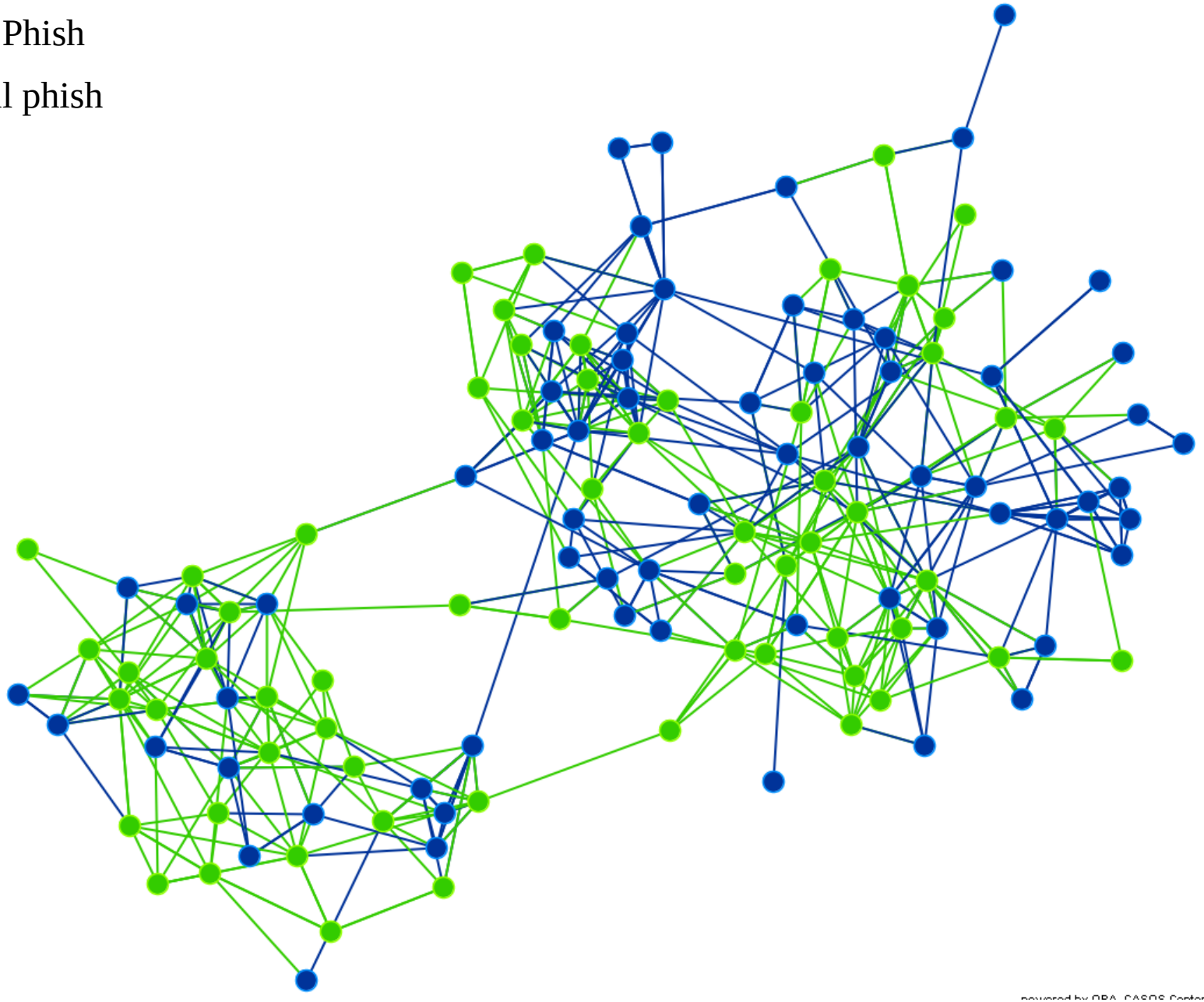
- Participants:
  - US Military Academy cadets, aged 18-25
  - One complete military unit (n=128)
  - 89% males
  - 30% freshman, 28% sophomore, 22% junior, 20% senior

- Security
  - 48% clicked the embedded link
  - 30% entered credentials
  - 5% warned others

FRIENDSHIP NETWORK

Failed Phish

No Fail phish

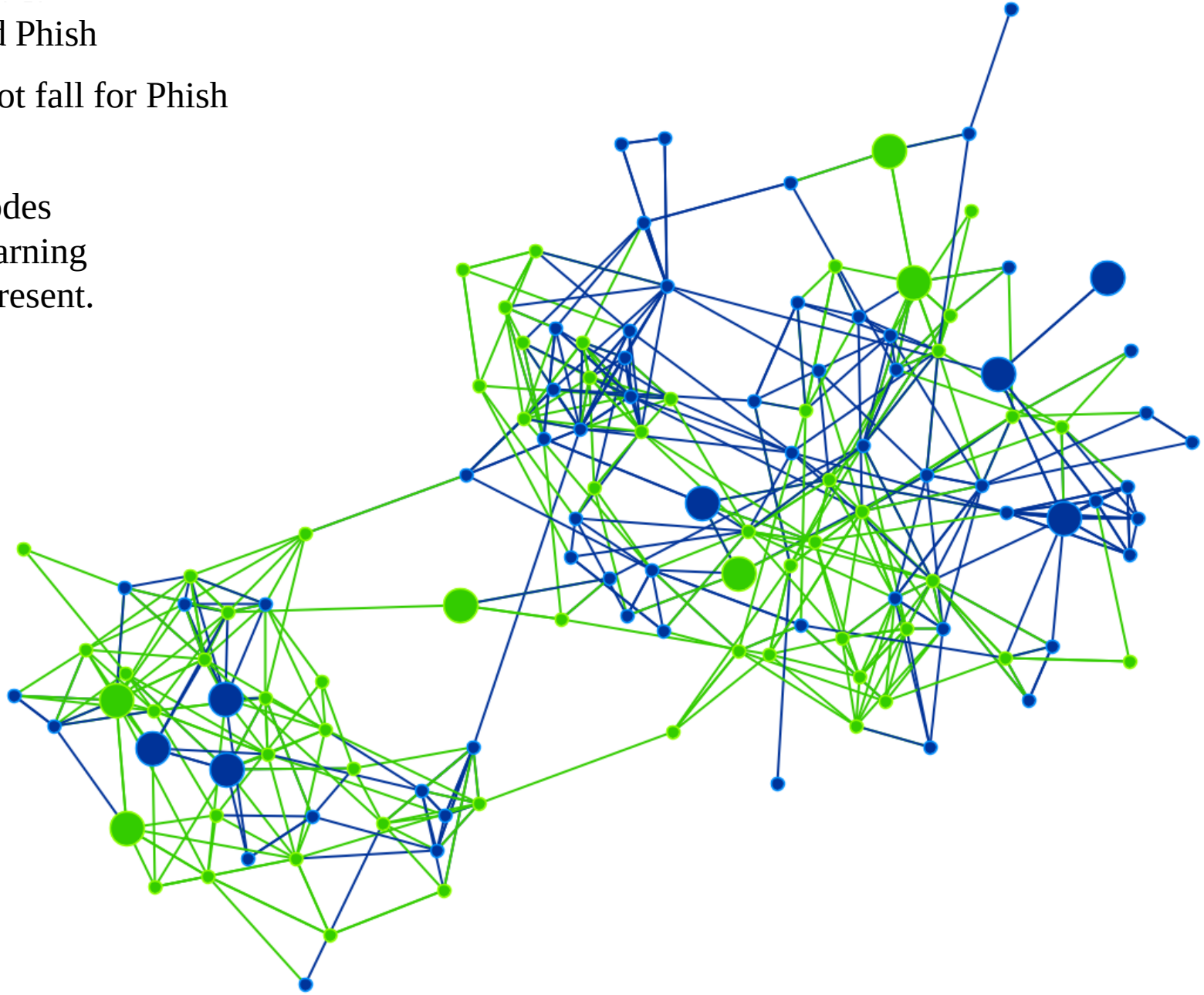


FRIENDSHIP NETWORK

Failed Phish

Did not fall for Phish

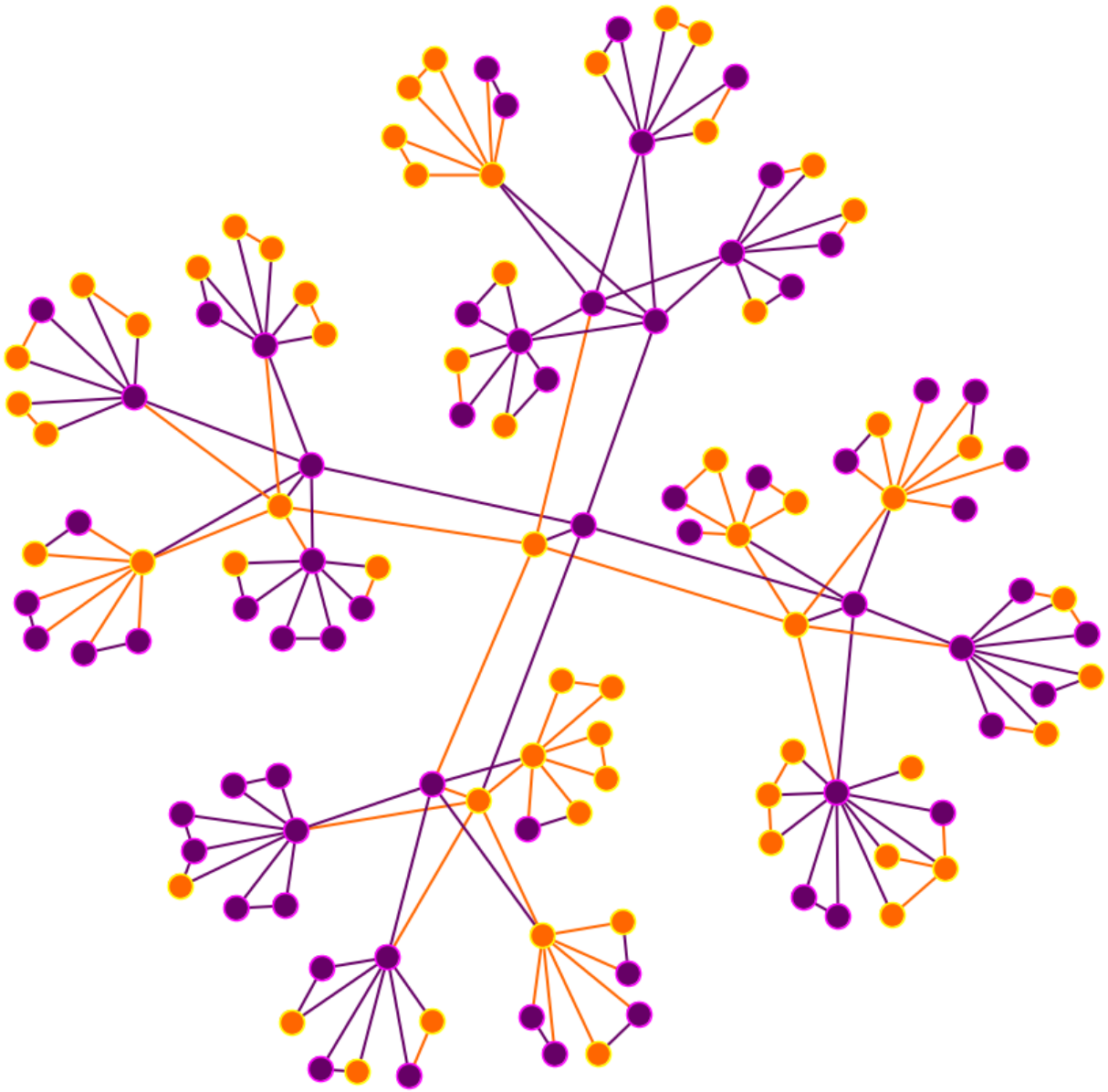
*Larger nodes indicate warning behavior present.



CHAIN OF COMMAND NETWORK

Failed Phish

Did not fall for Phish

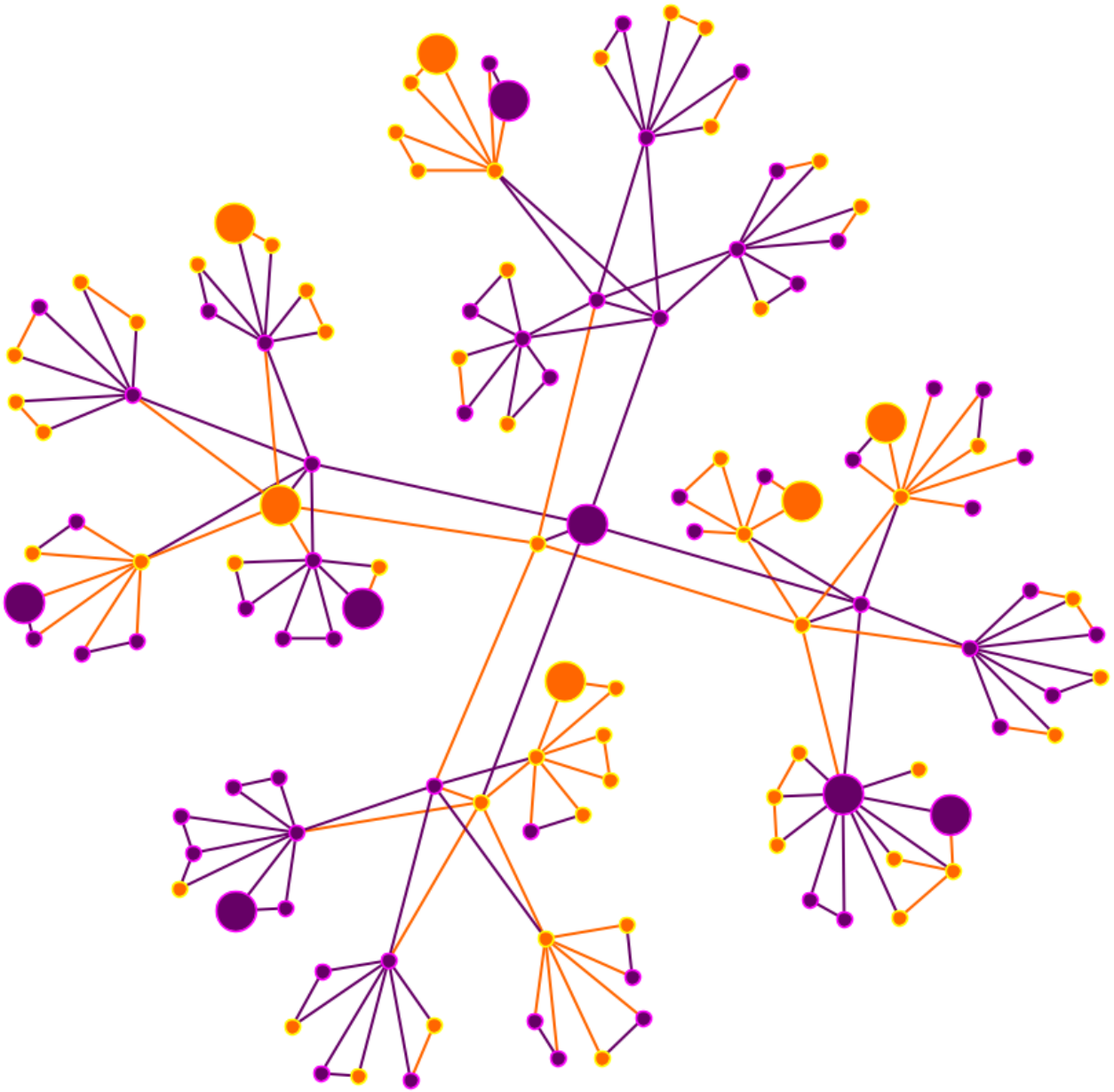


CHAIN OF COMMAND NETWORK

Failed Phish

Did not fall for Phish

*Larger nodes indicate warning behavior present.



Centrality

	Failure		Warning	
CENTRALITY	*Command*	*Friendship*	*Command*	*Friendship*
closeness	-0.05	0.08	0.23	-0.19
betweeness	-0.12	0.05	0.01	-0.02
eigenvector	-0.05	0.03	0.11	-0.17
indegree	0.08	0.05	0.04	0.06
outdegree	-0.12	0.16	0.02	-0.02

Command leadership correlates with:

- security resilience (decreased phishing failure)
- warning

Informal leadership correlates with:

- failure
- no warning

Local Network Homophily

Logistic Regression of Failure

	Odds Ratio	se	p-value
warn	1.21	0.75	0.754
male	1.17	0.70	0.795
class year	0.81	-0.15	0.235
CoC failure exposure	0.70	-0.12	0.033
CoC warning exposure	2.28	0.83	0.025
constant	1.62	1.16	0.496

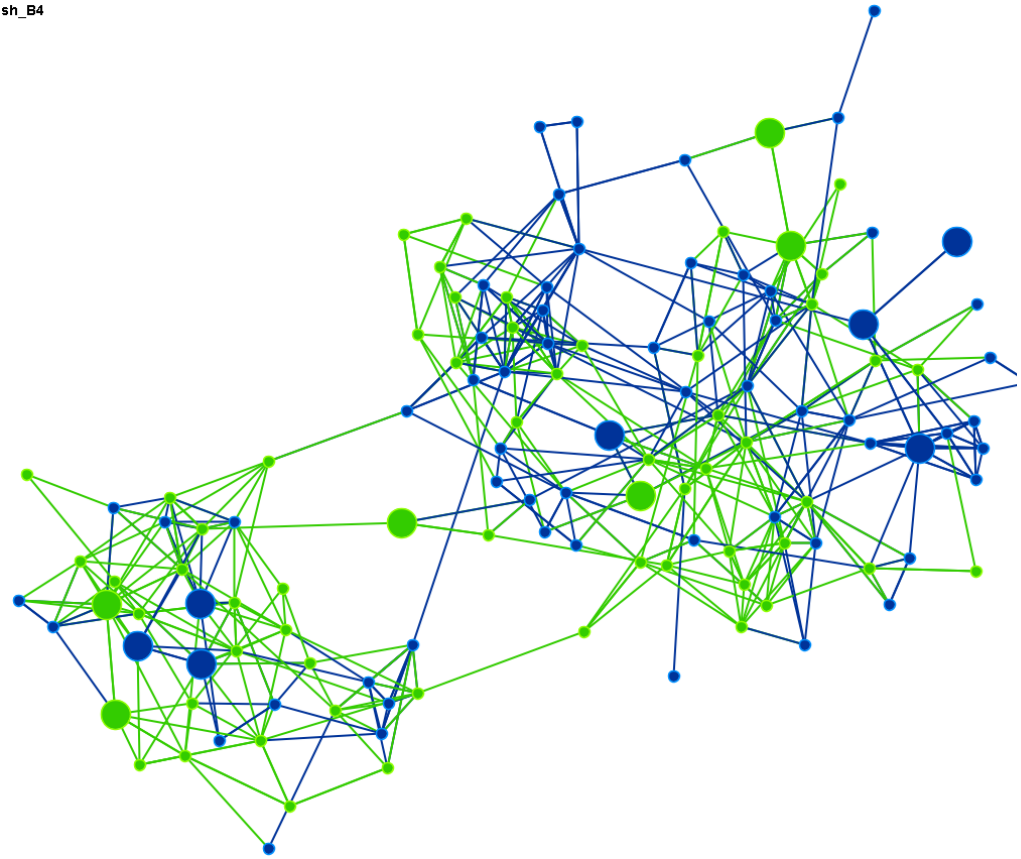
Logistic Regression of Warning

	Odds Ratio	se	p-value
fail	0.80	0.50	0.728
male	0.38	0.29	0.199
class year	1.00	0.28	0.996
friend warning exposure	2.32	0.89	0.028
constant	0.16	0.17	0.092

- *Command* relations are involved with *phishing vulnerabilities*
- *Friend* relations are involved with *warning behaviors*

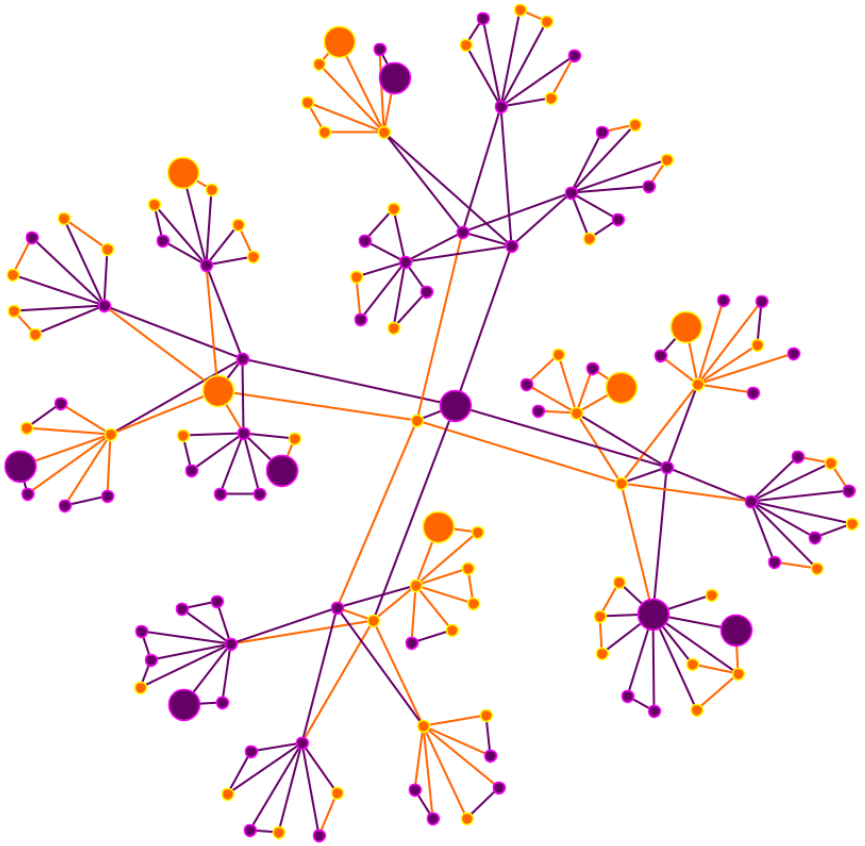
FRIENDSHIP NETWORK

sh_B4



Failed Phish

COMMAND NETWORK



Failed Phish

*Larger nodes indicate warning behavior present.

FRIENDSHIP & COMMAND

Failed Phish

Did not fall for Phish

*Larger nodes indicate warning behavior present.

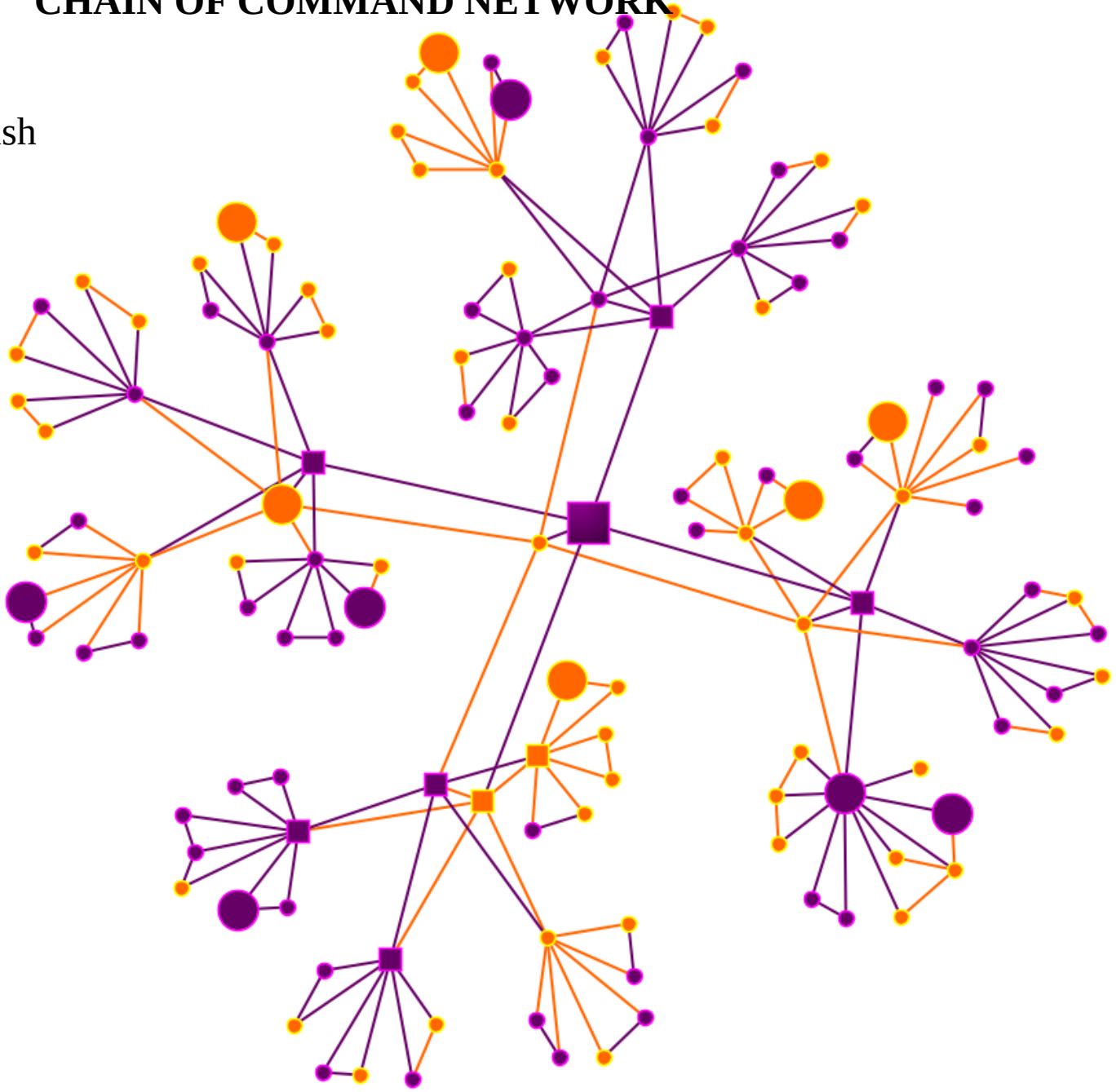
CHAIN OF COMMAND NETWORK

Failed Phish

Did not fall for Phish

*Larger nodes indicate warning behavior present.

*Square shaped nodes indicate friendship ties.



Structural Capabilities

- Friendship networks
  - Characterized as being highly centralized and clustered - few individuals have key roles in spreading information.
- Command networks
  - Have the potential to be very efficient - all individuals in the network can be reached with fewer number of steps (2 versus 5 steps, on average).

	Friendship	**Command Chain**
Link Count	600	198
Density	0.036	0.012
Average Distance	5.020	2.009
Betweenness	0.259	0.002
Closeness	0.042	0.708
Total Degree	0.058	0.036

Summary of Results:
Social determinants of Cyber Security

Informal Social Structure

1. Friendship leadership is vulnerable – more failure, less warning

2. Cyber risk resiliency among friends - while there is less **warning** among friends, there is homophily around this behavior

Formal Command Structure

1. Command leadership is strong – less failure, more warning.

2. Cyber risk vigilance among commanders/subordinates -- reduced security failures ego corresponds to higher **failures** and lower warnings in one's network.

Multiplex Relations

1. Trust improves security coordination -- Warning was likely given and headed among those who share friendship and command links

Future Work

- Security training and research should:
  - Emphasize the importance of security vigilance (failure) among formal leadership structures
  - Harness positive behaviors among informal relations (warning)
  - Further explore the role of multiplex relations in these settings
  - Utilize high betweenness in friendship network, and high closeness in command network

- Currently, conducting phishing study – 3 waves. Collecting network, org identity, and trust survey data.
- Understand other ideological, information exchange and contagion processes among formal and informal networks in military units – leadership, ideology, morale, leadership, performance.

Questions?

References

- Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why Phishing Works. Computer Human Interaction - Security, (pp. 581-590). Montreal.
- Heim, S. G. The Resonant Interface. Boston, MA: Pearson Education-Addison Wesley, 2008.
  Hicks, D. (2005). Phishing and Pharming: Helping Consumers Avoid Internet Fraud. Communities and Banking , 29-31.
- Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social Phishing. Communications of the ACM , 94-100.
- Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L. F., Hong, J., Blair, M. A., et al. (2009). School of Phish: a real worl evaluation of anti-phishing training. 5th Symposium on Usable Privacy and Security. SOUPS.
- Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., et al. (2007). Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit.
- Monitor, C. S. (2002). Poverty now comes with a color TV. Retrieved November 29, 2010, from MSN: http://webcache.googleusercontent.com/search?q=cache:RQYryc3YGVMJ:articles.moneycentral.msn.com/Investing/Extra/PovertyNowComesWithAColorTV.aspx
- Parrish, J. L., Bailey, J. L., & Courtney, J. F. (2009). A Personality Based Model for Determining Susceptibility to Phishing Attacks . Little Rock: University of Arkansas .
- Phifer, L. (2010, April 12). Top Ten Phishing Facts. Retrieved Novemeber 29, 2010, from eSecurity Planet: http://www.esecurityplanet.com/views/article.php/3875866/Top-Ten-Phishing-Facts.htm
- (2009). Phishing Activity Trends Report. Anti-Phishing Working Group .
- Sheng, S., Holbrook, M., & Kumaraguru, P. (2010). Who falls for a phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. 28th International Conference on Human Factos in Computing Systems . Atlanta: CHI.